(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 February 2001 (01.02.2001)

PCT

(10) International Publication Number
WO 01/08116 A2

(51) International Patent Classification[7]: G08B 21/00

(21) International Application Number: PCT/GB00/02880

(22) International Filing Date: 26 July 2000 (26.07.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
9917490.6 27 July 1999 (27.07.1999) GB

(71) Applicant *(for all designated States except US)*: ACTIVERF LIMITED [GB/GB]; Downing Park Innovation Centre, Swaffham Bulbeck, Cambridge CB5 0NB (GB).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: BEART, Pilgrim [GB/GB]; Russell House, Chippenham Park, Chippenham CB7 5PT (GB). BEART, Jason [GB/GB]; Highfield Farm House, 11 Apthorpe Street, Fulbourn, Cambridge CB1 5EY (GB).

(74) Agent: HARRISON GODDARD FOOTE; Tower House, Merrion Way, Leeds LS2 8PA (GB).

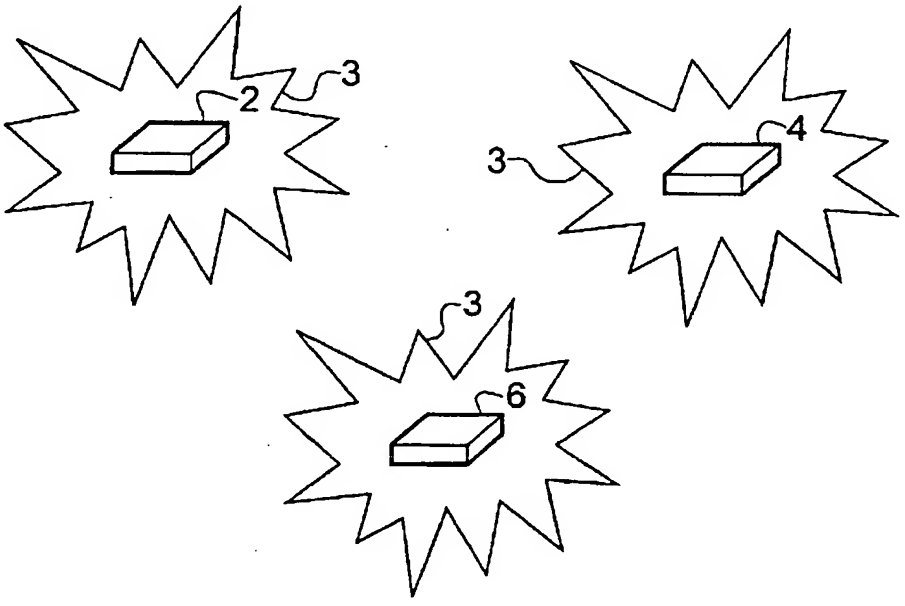
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *Without international search report and to be republished upon receipt of that report.*

[Continued on next page]

(54) Title: IMPROVEMENTS RELATING TO SECURITY



(57) Abstract: A security system comprising a plurality of units (2, 4, 6), each being provided with a power source, a processor (U_1), a transmitter (TX_1) and a receiver (U_2), and at least one of the units further being provided with an alarm (H). The units (2, 4, 6) are operable to communicate with each other by way of the transmitters (TX_1) and receivers (U_2), and the processor (U_1) is adapted to generate an alarm signal in the event that certain communication events occur.

WO 01/08116 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

IMPROVEMENTS RELATING TO SECURITY

This invention relates to a new security system and a method of providing security.

It is well known that it is desirable to provide security for various types of articles. For example items of high value, high intrinsic value, of sentimental value, children, pets, may all need to be guarded.

There are many known security systems which aim to provide security for objects. As will be appreciated each of these existing systems has its own separate advantages and disadvantages. One of the most basic systems is provided by locking the articles in place. This is simple but effective and yet is easy to overcome if the correct tools are available. Further, such an approach is not applicable to certain situations, for example guarding children in a playground and other similar situations.

It is also known to provide an alarm in association with each item that is being guarded. Such an alarm may be activated by motion, tampering, removal of the article, etc. Again, such a system would not be suitable for guarding children within a playground, or guarding a collection of articles which are moved from place to place (for example a group of suitcases). These systems are vulnerable to attack on each of the alarms, ie the individual alarm can be muffled, or broken to prevent it from sounding.

Further, so-called burglar alarms are well known wherein sensors are provided which are connected to a centralised alarm system. Once again such systems cannot provide protection for objects which are mobile (for example collections of bags, groups of children). Further, such centralised alarm systems are vulnerable to an attack on the centralised alarm system.

According to a first aspect of the invention there is provided a security system comprising at least two units, each unit comprising a power source adapted to power

the unit, a processor, a transmitter, a receiver and at least one of the units having an alarm, the units having the ability to communicate with each other via the transmitters and receivers, the processors being adapted to control the units and to cause the alarm to generate an alarm signal when predetermined rules are satisfied.

Such a system is advantageous because it allows a unit to be applied to an article to be guarded. Because the system relies on communication between the two units there is no central control system open to attack and each unit must be individually disabled to disable the security system as a whole.

In one embodiment, at least one processor is adapted to generate an alarm when communication fails between the two units, providing a simple system. As will be appreciated the predetermined rules may cover a number of situations, some of which are outlined hereinbelow.

In one arrangement if one of the units is disabled then the other will lose communication with it and an alarm will be raised. If an article to which one of the units is attached is simply removed then eventually it is likely that it will be taken beyond the communication range of the units (or an obstruction will intervene) and again communication will fail allowing an alarm to be raised, if communication failure is a predetermined rule.

Preferably there are more than two units, each of which has the ability to communicate with all the other units of the system. This is advantageous because it will allow more than two articles to be guarded with a single unit being provided for each article.

Each of the units in the system may be adapted to generate an alarm when predetermined rules are met, which may be when communication fails with any one of the units or when the distance from any one of the units exceeds a given value. This is advantageous since an alarm will emanate from each of the units even if only

one of the units has been stolen, run away, etc. causing the predetermined rules to be met.

The alarm may be provided by one or more of the following: a sound or vibration generating mechanism (eg a piezo electric sounder or other electric sounder), a light emitting device, a display screen, an electric shock generator, an explosive device, an electromagnetic lock or catch, or by signalling to a connected or remote (e.g. wireless) apparatus.

In an alternative embodiment only some of the units are provided with an alarm. An advantage of this is that it may be cheaper to realise than providing an alarm with each unit. The units may also be smaller and more convenient. In such an embodiment a unit provided with the alarm may be thought of as a master unit.

The transmitter of at least one of the units may be adapted periodically to transmit a signal, this being advantageous over continuous transmission because it is more power efficient. Of course, it would be equally possible to provide a transmitter which transmitted a signal continuously. Further, the receiver may be powered periodically and therefore capable of receiving a signal periodically.

The skilled person will appreciate that two initially in-phase uncorrelated periodic signals will gradually drift out of phase. Therefore, should two units simply communicate at predetermined intervals, eventually the units may drift apart so that no receivers are listening when a transmission occurs. Therefore, the processor of one of the units may be adapted to control when the transmitter transmits signals and may be adapted to operate the transmitter when the receiver of another unit is activated to receive a signal. Alternatively, or additionally, the processor may be adapted to control when the receiver receives signals and may be adapted to operate the receiver when the transmitter of another unit is transmitting a signal. The processor may be adapted to learn when transmission is expected and only activate the receiver at this time. The receiver may be adapted to be powered and capable of

receiving a signal for a period either side of when a signal is expected so increasing the likelihood of receiving the signal.

Further, the transmitter may be adapted to transmit pieces of information, which may include any from the following list: the identity of the unit from which the communication originated (unit identification), the class of unit from which the communication originated, the level of output from the power source of the unit, the status of the unit, when the next transmission will occur. Each of these pieces of information has its own separate advantages. For instance it is advantageous to transmit the unit identification so that the remaining units of the system can tell from where the transmission originates. There may be a number of different classes of unit within the security systems which may have one or more units within them. Units within the systems may be adapted to have different responses depending upon what class of unit they are in communication with.

Transmission of the level of output power from the power source is advantageous in that it helps to prevent false alarms through power source failure. Clearly, if a power source fails the unit will stop transmitting. Generally, such a lack of transmission would cause the remaining units to generate an alarm. However, the processors of the units may be adapted to suppress the generation of an alarm if a unit stops transmitting after a period of reporting low power source levels. The processors may be adapted to warn the user of a low power source before that power source fails.

The processors of the units of the system may be adapted to generate an alarm if one of the units transmits a status signal indicating that an alarm should be generated.

Preferably the transmitters and receivers are respectively adapted to transmit and receive radio signals. Such a medium is advantageous because it is generally omni-directional, will pass through a number of obstructions (ie does not necessarily require line-of-sight communication) and has a finite range. It is advantageous to

have a finite range because for some embodiments of the system to function, communication must eventually be lost if one of the units is removed.

In one embodiment the transmitters and the receivers are adapted to operate at substantially 433MHz. Such a frequency is advantageous because it is an unlicensed frequency (not requiring a licence to use) and will thus be readily available for such use. The skilled person will appreciate that the system may operate using any radio frequency and that 433MHz is merely one embodiment.

The units may communicate with each other using standard frequency-based communications, including frequency modulation and amplitude modulation. Where digital signals are used, frequency shift keying (FSK) or amplitude shift keying (ASK) may be appropriate, or frequency-hopping or spread-spectrum. Alternatively, time-modulated ultra-wide band (UWB) communications technology may be employed, in which precisely timed (possibly down to picosecond resolution) extremely short pulses are used to transmit digital data over a wide range of frequencies.

In an alternative embodiment, the transmitters and the receivers are adapted to communicate short pulse signals to each other. The pulse signals will generally be unmodulated, that is to say, not capable of transmitting information other than an indication of the presence of a unit. The processors of the units in this embodiment are preferably adapted to expect to receive pulse signals from predetermined other units at predetermined times or periods of time, thus providing a simple method of determining the presence or otherwise of a given unit within the system. Furthermore, the processors may be adapted only to activate the receivers when a pulse is expected, thereby helping to reduce power consumption. As a development of this communications protocol, the units may undergo an initialisation stage in which, say, modulated RF data packets are transmitted and received at predetermined times and intervals, the data packets including information serving to identify the respective transmitting unit to the other units. Once the processors of the various

units have learned the expected pattern of times and intervals, pulse signals (say, a few cycles at a given operating frequency, e.g. 433MHz) rather than full data packets may be transmitted so as to indicate the presence of each unit within the system. This process may be continuously controlled by a slowly-clocked CMOS integrated circuit, thus further helping to reduce power consumption.

In some embodiments the transmitters and receivers have a range of about 1m to 150m, perhaps about 30m to 125m. In one embodiment the transmitters and receivers may have a range of about 100m. In an alternative embodiment, the transmitters and receivers may have a range of 5m, 10m or 20m. It will be apparent that, for embodiments which generate an alarm when communication fails, the range of transmission is a compromise between providing a degree of freedom of movement for each of the units but providing a relatively short distance before communication fails between units and an alarm is generated. If the range is too short alarms will be generated too easily and if the range is too long a low degree of security will be provided since too much freedom will be given to the units.

In other embodiments, the range may be several kilometres (may be substantially 1, 2, 3, 4, 5, 6km or more). Such ranges are advantageous for providing security for items which in general use are separated by distances of these orders. An example of such items would be farm machinery. The skilled person will appreciate that the range must allow the item to perform its usual function without the generation of false alarms.

The receiver of at least one of the units may comprise a detector adapted to detect communication from another unit. In normal operation the unit may be adapted to operate in a low power state and be further adapted to become fully operational when the detector detects a possible communication. It will be appreciated that in the low power state some power may actually be drawn from the power source. A detector which allows the units to operate in a low power state is advantageous because it increases the life of the power source. The at least one unit may be adapted to

become fully operational for a predetermined period of time upon detection of a possible communication. Alternatively or in addition, the at least one unit may be adapted to return to the low power state upon detection of a "sleep" communication directed either generally to all of the units or to that particular unit.

The power source may be a battery which provides a convenient source of power. The battery may or may not be rechargeable. Alternatively, or additionally, a solar cell or a Peltier junction may provide the source of power. A capacitor may be provided in association with the solar cell, allowing power fluctuations in the output of the cell to be smoothed.

Alternatively, or additionally, power may be derived from an external power supply, which may or may not be permanently wired to the unit. An example of this would be a charger or mains wiring. In another alternative or additional embodiment power may be derived via electromagnetic coupling or induction from a nearby coil or antenna, which may be provided on a nearby anchor unit. Power may also be provided from motion via an electric generator or piezo generator.

At least one and preferably each unit of the system may be provided with an identification mechanism adapted to provide unit identity. The processor of at least one of the units may be adapted to interact with the identification mechanism and transmit the unit identity via the transmitter. Indeed, the identification mechanism may be a part of the processor. As discussed hereinbefore this is advantageous so that each unit can identify itself to the other units of the system, and units receiving transmissions will know from where the transmission originated. The identification mechanism may provide a unique identification for a particular unit or may identify a unit as belonging to a particular class. Indeed, in some embodiments the identification mechanism may provide both a unique identification and also a class of membership. Providing a class membership is advantageous because it allows the units of the system to behave differently when communicating with units of different classes. Further, because a class of membership is not unique to a particular unit, the

communications could not be used to invade privacy as could communications involving a unique identification.

The units may further comprise an arming mechanism adapted to cause the unit to become operational. The arming mechanism may comprise a key-receiving mechanism adapted to receive a key. The key-receiving mechanism may be adapted to receive any one of the following: an electronic key (for example a smart card or similar), a mechanical key, an arming code transmitted to the unit and received by the receiver.

One or more units of the system may comprise an arming unit adapted to arm the system. The arming unit may be adapted to transmit an arming code which arms and/or disarms the remaining units of the system. When the system comprises a master unit having an alarm, the master unit and the arming unit may be the same unit. In an alternative embodiment the master unit and the arming unit may comprise separate units.

In an alternative embodiment the master and/or arming unit may be adapted to transmit a suppression signal adapted to prevent the units of the system from arming. The units of the system may be adapted to arm if they do not receive the suppression signal for a predetermined period. It will be appreciated that in a different embodiment the suppression signal may prevent the units of the system from disarming and keep them armed when they are receiving the signal.

Alternatively, the system may become armed when the power source of each unit is connected.

Where an arming unit is provided it may be adapted periodically to change the arming code. An advantage of this is that it prevents the arming code being copied and fraudulently used by a third party to arm or disarm the system. The skilled person will appreciate that algorithms for securely changing a code are well known.

Further, it will be appreciated that if the code is to be changed, the units receiving the arming code must alter the code they are expecting to receive in the same manner as the unit transmitting the arming code. An example of such an algorithm is the Keyloq™ protocol.

The units may be adapted to encrypt communications. An advantage of encryption is that system security is increased. Encryption algorithms will be well known to the person skilled in the art but may include public-key or challenge response algorithms. When the units are encrypting the communications a single communication may become several transmissions, encoded for each recipient unit.

The unit may be provided with a memory. The processor may be adapted to store within the memory the identities of the units with which it is in communication. Remembering the identities in this manner allows the system to track the units within the system. In embodiments where an alarm is generated when communication fails, tracking the units of the system will allow the unit to know when one of the units is no longer in communication, indicating that an alarm should be raised.

The processor may be adapted to store a log of events within the memory. An event may be any action of which the unit becomes aware for example: a reading from a sensor, the contents of communications received from other units, the time at which the event occurs, etc. The processor may be capable of causing the transmitter to transmit all or some of the contents of the log and/or memory. The processor may be adapted to cause such a transmission when a predetermined communication is received, or at predetermined times, or after a predetermined sensor input, etc.

The processor of a particular unit may be adapted to store in the memory only the identity of those units which are in communication with the particular unit at a certain time or during a certain period. The period may be within a predetermined period of the system becoming armed. This is advantageous because it prevents the units, including units which are not part of the desired security system, from being

included in the security system. The system is designed to guard articles to which the units are attached using communications between the individual units. Clearly, any unit of substantially the same design is capable of communicating with the units of the system. If units are simply included into the system as and when they come into communication then the system could guard articles which it is not intended to guard (that is articles fitted with units which can communicate with units of the system). Only remembering the identity of some units has the advantage that units which should not be included into the system will not be included into the system.

In an alternative embodiment the units may be adapted to generate an alarm if a communication is received from a unit having a particular identification or from a unit belonging to a particular class. This is advantageous because it could be used to enforce an exclusion order against a party. For instance, that party may be provided with a unit having a known identification and other units situated in an excluded area may be programmed so that if they detect the known identification an alarm is generated. In another example, a lift may be provided with a unit and passengers may be provided with units belonging to a class defined as passengers. The unit provided on the lift may count passengers into the lift and generate an alarm once the number of passengers exceeds a predetermined limit. A further example would be to exclude visitors from restricted areas of a premises. An alarm may be generated should the presence of a unit belonging to a visitor be detected.

The predetermined rules may be arbitrarily complex and may be based upon a number of parameters which may include any of the following: state of external sensors, the presence/absence of particular unit identities, presence/absence of units belonging to a particular class, contents of communications from other units, data held within the processor and/or memory.

The processor may be provided with an input device adapted to program the processor with the identity of units which are part of the system. As discussed in the previous paragraph this is advantageous because it will prevent units which it is not

desired to guard entering the system. In another embodiment the identities of units which are in communication with a particular unit are stored in the memory whilst the input device is activated. The input device may be a button, switch, a keyboard, a collection of keys, etc. In use, a user may activate the input device for a period, during which time the processor stores the identities of units with which it is communicating.

The predetermined rules which define when the processor is adapted to generate an alarm may be alterable by a user. The input device may be further adapted to allow the rules to be changed. Clearly, this is advantageous because it will allow the functionality of the system to be altered to suit the current requirement. Alternatively, or additionally, the processor may be adapted to alter the predetermined rules upon receipt of a predetermined communication from another unit. The processor may be adapted to change the predetermined rules on the basis of events.

At least one of the units may be provided with other sensors whose outputs are connected to the processor. The processor may be adapted to monitor the outputs from these sensors and may be further adapted to transmit information relating to the sensor output to the transmitter. For instance, the sensor may be adapted to generate a signal within an allowable range and the processor may be adapted to cause the transmitter to transmit a signal if the signal from the sensor falls outside this allowable range. In another embodiment the sensor may be adapted to generate a signal only on the occurrence of a certain circumstance and the processor may be adapted to cause a signal to be transmitted by the transmitter only when a signal is produced by the sensor.

Examples of sensors which may be provided are: moisture sensors, motion/tilt sensors, tamper switches, continuity-loop sensor wires from external alarm systems, signals sent from a computer program running on an attached computer, signals sent from a co-located "RFID" chip, co-ordinates from a Global Positioning sensor,

signals from a mobile phone, a magnetic field sensor such as a compass, a biometric sensor and a physiological sensor. Of course any other type of sensor could be provided.

At least one of the units may be provided with a connector to connect the unit with apparatus remote from the security system. For example the connector may be adapted to allow communication with any one of the following: a video display, a web site, a telephone system, a computer network, a portable computing device, a mobile phone network, a door lock, a turnstile, another security system (which may be as defined herein). This list is not intended to be exhaustive and the skilled person will appreciate it may be desirable to allow the unit to the connected to a variety of other apparatus. The connector may be adapted to make available the status of the security system. The connector may be adapted to transmit the contents of the memory and/or log to the device to which the unit is connected.

Preferably the units are provided with an attachment device adapted to attach the unit to an article to be guarded. Alternatively the unit may be built into the article to be guarded. Clearly, security will be increased if the units can be securely attached to the unit to be guarded.

In one embodiment the unit is provided as one of the following: a tag, strap, necklace, belt, wristwatch, bracelet. The unit may be adapted to be worn by a user. Such embodiments are useful for guarding a collection of people, which may be children. A party of people could then be guarded and an alarm would be raised should one of the party move out of communication range, perhaps by becoming disorientated and lost or perhaps due to abduction, etc.

The system may comprise an anchor unit. The anchor unit may have the functionality of a unit of the security system. The anchor unit may be attached to a substantially permanent structure. Such an anchor unit is advantageous because it may allow units to be attached to and guard highly portable articles. It will be

realised that the alarm will only be raised if the predetermined rules are met, perhaps a unit of the system loses communication with the remaining units of the system. Therefore, should all of the units in the system be attached to highly portable articles which are all removed at once no alarm might be raised. Providing an anchor unit is advantageous because it should prevent all of the units from being removed at once. A plurality of anchor units may be provided.

The processor may be a microprocessor or may be a micro-controller. In one embodiment the micro-controller may be from the PIC series from the Micro-Chip Corporation. In another embodiment the processor may be provided by an ASIC, possibly providing lower power consumption than may be obtained from a microprocessor or micro-controller.

In one embodiment the transmitter may be an LQ-TX433A-S manufactured by LPRS Ltd. In an alternative embodiment the transmitter may be provided by transistor oscillator or other electronic circuit which may be stabilised using a SAW (Surface Acoustic Wave) device or crystal.

The transmitter may be adapted to provide one of the following modulation formats which may be advantageous due to increased range and reliability of the system: on-off keying, amplitude shift keying, frequency shift keying, frequency modulation, amplitude modulation, frequency hopping, spread spectrum and time-modulated ultra-wide band.

The receiver is preferably a circuit providing the function "radio in, data out". An example of such a circuit is the MICRF-00x series from the Micrel Corporation.

Alternatively, the transmitter and the receiver may be provided in a single transceiver. For example an ASH transceiver from RF Monolithics Inc. may be provided. Indeed, the transmitter, the receiver and the processor could all be

provided on the same circuit, for example the BlueCore Single Chip Bluetooth Modem designed by Cambridge Silicon Radio Ltd.

An antenna may be provided to transmit radio signals. The antenna may take any one of the following designs: whip (wire, PCB stub, or PCB spiral), wire helix (or combined whip and helix), loop (wire, or PCB, open or closed), dipole, slot, patch, dielectric resonator antenna or metal part of the attached object. Preferably, the antenna is a ¼ wavelength in length. Conveniently the antenna is tuned to resonate at the operating radio frequency. The skilled person will appreciate that the preferred embodiment will depend on the operating frequency and space constraints of the application.

The same antenna may be used by both the receiver and transmitter, or alternatively separate antennas may be provided for the transmitter and the receiver.

In one embodiment two antennas are provided in a unit increasing the reliability of the signal transmission. The skilled person will appreciate that signals transmitted from an antenna do not radiate equally in all directions. The orientation of a unit will be unknown and therefore other units may lie in areas which do not receive a substantial signal from a particular antenna (ie there is no or little signal transmitted in that direction). Should two antennas be provided they may be positioned at substantially 90° to one another, or may be positioned at some distance from one another. The antennas may be used alternatively for transmission and reception. These techniques are advantageous due to increased coverage of the radio transmission and reducing possible blind spots.

In some embodiments the antenna system may comprise an array of antennas in one of various "beam-forming" or "radio direction finding" RDF configurations well known to those skilled in the art. This allows the unit to monitor the positions of other units from which it receives communications. The processor may be adapted to use this information to generate an alarm in certain circumstances. For instance an

alarm may be generated if the direction of one of the units with which the unit is in communication with moves beyond predetermined limits. Alternatively, or additionally, the array of antennas may be used to beam communications substantially only in the direction of the intended unit.

According to a second aspect of the invention there is provided a method of providing security comprising providing at least two units capable of communicating with each other using transmitters and receivers, the method comprising sending communication signals between the two units and raising an alarm when predetermined rules are satisfied.

Such a method is advantageous because it provides decentralised security in which each of the units must be disarmed in order to disable the security.

The method may generate an alarm when communication fails between two units.

Preferably the units are attached to articles which it is desired to guard. Conveniently, the method includes providing a plurality of units, preferably one for each article which it is desired to guard.

The method may comprise providing an arming mechanism to arm and/or disarm the system which is advantageous because it provides controllability over the method.

The method may comprise providing a master unit (or arming unit) which transmits a suppression signal which prevents the units of the system from arming. The units/system may automatically arm in the absence of the suppression signal. This is advantageous because it may allow the system to automatically arm if the master unit were moved outside the transmission range of the remaining units; for example if a person carrying the master unit moves away from units to be guarded by the security system. The system may not require guarding if the person with the master unit is in

the vicinity of the remaining units. The method may comprise providing more than one master and/or arming unit.

The system may perform a communication check. Such a check may be initiated by a unit, which may be the master unit. The communication check may cause each of the units to communicate. Such a check is advantageous since it gives the user knowledge that the system is working. A communication check is especially advantageous in situations where there is likely to be poor communication, perhaps in the vicinity of large radio or radar transmitters, or may be used to detect if jamming is occurring.

In one embodiment, the method comprises causing each unit to remember the identity of all of the units with which it is in communication when the system is armed or may be within a predetermined period of the system being armed. This has the advantage that the units which are not part of the system but which are capable of communicating with the units (perhaps on neighbouring systems) do not become included in the method (unless they are in communication when the system is armed).

Alternatively, or additionally, a different method may be provided for determining which units form part of the security system. An input device may be provided which may be used to input the identity of units which form part of the security system. Alternatively, or additionally, the units may remember with which units they are in communication when an input is made to an input device. Each of these methods provides a convenient way of restricting the units which are protected by the method.

The method may comprise causing the units to transmit signals at predetermined periods. This is advantageous because it reduces the power consumption of the units.

The method may comprise causing the units to receive signals periodically. Again this is advantageous because it means that power consumption is reduced. Preferably, the units receive signals when a signal is being transmitted and the method may comprise techniques to ensure that transmission and reception occur at substantially concurrent times to ensure that transmissions are not lost.

Preferably the units transmit their status, which may include the status of a power source. This is advantageous because it allows the failure of power sources to be taken into account and thus, possibly reduce the generation of false alarms. The skilled person will appreciate that if a power source fails the unit which it is powering will stop transmitting generally resulting in an alarm. However, the method may include the step of suppressing an alarm signal if a unit stops transmitting after a period of reporting a low power source.

Preferably the method also includes noting the signal strength of transmissions received form units. This again may help to reduce the number of false alarms. If it is clear that one of the units is on the fringes of a receivable signal range, it may not be surprising if it drifts in and out of communication. Therefore the method may include the step of suppressing an alarm if communication is broken to a unit which has been experiencing a weak signal strength. The skilled person will appreciate that such a step is a compromise between reducing the security offered and reducing the number of false alarms. Clearly, if the method is made too tolerant of weak signals it would become possible slowly to remove a unit so that it begins to experience reception problems and finally to remove the unit completely thus fooling the system.

Further, each of the units may estimate the range of the other units in the system with which it is communicating. This estimation may be performed by measuring the signal strength of the signal received from other units or by measuring the time-of-flight. The method may comprise causing a particular unit to ignore units which are greater than a predetermined range from the particular unit. As discussed in the previous paragraph this is advantageous because it helps to reduce the likelihood of

false alarms. The skilled person will appreciate that as the range increases the received signal strength will fall and that ignoring units above a threshold distance effectively ignores those with a less than acceptable signal strength.

Additionally or alternatively the method may provide a warning to a user that one of the units is experiencing a weak signal strength, or may be that one of the units is greater than the predetermined distance. This is advantageous because it allows the user to alter the position of the units such that all of them are within good communication range of each other.

The method may include providing tolerance to missed transmissions. The alarm may be activated if more than a certain number of transmissions are missed. This is advantageous because it may reduce the number of false alarms.

Examples where the method may be used include guarding pictures within a gallery. Each picture may be fitted with a unit communicating with the other units of the system. If one of the pictures were to be stolen, the alarm may activate as disclosed herein.

Another possible use of the method would be to guard skis, golf clubs, etc. which could be left outside lodges, or to guard farm equipment.

According to a third aspect of the invention there is provided a security unit comprising:

a transmitter for transmitting a signal;

a receiver for receiving such a signal when transmitted by a second, substantially identical, unit;

an alarm generator;

a processor adapted to activate the alarm generator according to a predetermined condition relating to the receipt or otherwise of a said signal.

For a better understanding of the present invention and to show how it may be carried into effect, reference shall now be made, by way of example, to the accompanying drawings, in which:

FIGURE 1 is a schematic of a security system according to the invention;

FIGURE 2 is a circuit diagram for realising a unit of the security system of Figure 1;

FIGURES 3 AND 4 are schematics of further examples of security systems realising the invention; and

FIGURE 5 shows a block diagram of a unit of the security system.

A security system comprising a number of units 2, 4, 6 is shown. Each of the units comprises a transmitter 8 (in this case a LQ-TX433A-S from LPRS) capable of transmitting radio waves of substantially 433MHz with a power of 1mW and a receiver 10 (in this case a MICRF-001 capable of receiving radio waves of substantially the same frequency. The operation of the transmitter and receiver 8, 10 is controlled by a processor 12 (in this case a PIC12C508 micro-controller) which is provided with a memory 14. The processor 12 is also connected to an alarm 16, in this case a piezo-ceramic element. The components of the unit 2, 4, 6 are powered by a power source 18, in this case two lithium coin cells in parallel generating substantially 6 volts.

The processor 12 receives binary data from the receiver 10 and also receives an output from a Received Signal Strength Indication (RSSI) output of the receiver 10. The RSSI output is particularly useful as will be appreciated from the discussions hereinafter. The processor 12 sends binary data to the transmitter 8. The skilled person will appreciate that the rate of transmission need not be high and will be dependent upon the components used. In this particular embodiment rates of substantially 1kbps were used.

An antenna (not shown) comprising a printed circuit whip tuned via capacitance to a ground plane on the opposite side of the circuit board is provided for signal transmission/reception.

In some embodiments the receiver comprises a detector which is permanently operational whilst the remainder of the electronics within the unit is in a substantially zero power state. The detector monitors for possible communications from other units and if such a communication is received fully powers the remainder of the electronics such that if the communication is a genuine communication it can be received by the receiver and processed by the processor.

In one embodiment, each of a collection of articles to be guarded is provided with a unit 2, 4, 6 according to the invention, the units being securely attached to the articles. An example of a collection of articles which may be guarded using the system is a collection of suitcases.

Once the units 2, 4, 6 of the system are armed the processor 12 causes the transmitter 8 periodically to transmit a signal. The signal contains the identity of the unit making the transmission (which is held within an identification mechanism (not shown) of the unit). The status of the battery 18 is also transmitted. Periodic transmission is beneficial because it will increase the life of the battery 18.

Possible schemes which may allow the periodic transmission to work are as follows:

Each unit has a fixed transmission period, eg once every 30 seconds. Initially the receiver of a particular unit is powered continuously until a transmission has been received from each other unit. Then the receivers simply turn-on shortly before each subsequent communication is expected from other units.

In order for systems comprising more than 2 units to function properly, each unit must have a different transmission period to avoid the danger of transmissions repeatedly colliding. One way of achieving this is to make each transmission-period "relatively-prime" to all the others, so that there is a low chance of two communications occurring at the same time.

Another way of achieving this is to "dither" the transmission time of each unit according to some complex, perhaps pseudo-random, algorithm, between limits (eg between 6 seconds and 30 seconds). Many such algorithms are possible, for example sets of linear-feedback shift-registers, with the feedback taps chosen uniquely for each unit to minimise the number of successive collisions that are possible in the system as a whole.

In such a pseudo-random scheme the transmission period changes on each transmission. The receiver can either have a duplicate algorithm to allow it to predict the next transmission time from each remote unit, or the "time to next transmission" can be encoded in the transmission itself.

If communication is lost, the unit may attempt to re-establish communications by occasionally reverting to the initial state of "receiver always on" for the maximum allowable transmission period, during which it should hear from all other units at least once.

It will be appreciated that the transmitted data could be provided in any number of formats. However, in one embodiment each bit of the packet is bi-phase encoded, meaning that each bit-period starts with a transition (low-to-high or high-to-low) and "one" bits have an additional transition in the centre of the period. Further, the data packets may include any of the following parts:

A preamble which allows the receiving means 10 to adjust its Automatic Gain Control (AGC) to enable proper decoding of the rest of the packet. It will be

appreciated that the early part of the preamble may well be lost whilst the AGC corrects its setting.

After the preamble the packet may comprise a break, or silence, which may be longer than an allowable bit period. This allows the receiver 10 to recognise the following bit as the start of valid data.

After a break, two bytes of data are sent. The first byte contains an identification code and the second byte contains the status of the unit.

In some embodiments the communications between the units are encrypted thereby further increasing the security of the communication. For instance, public-key or challenge-response algorithms may be applied to the communications.

As can be seen from Figure 1 each of the units 2, 4, 6 transmits such a signal 3. The transmissions from each of the units 2, 4, 6 are received by the receiver 10 and the received signal is processed by the processor 12.

The units 2, 4, 6 have a relatively low power and therefore the transmitted signal has a range only in the order of tens of meters. Consequently units separated by more than this distance will not be able to communicate with one another. Of course, in other applications the units may have a range of the order of kilometres.

Each unit will know how many other units there are in the security system from data stored in the memory 14 and will expect to receive a signal from each of the other units. If, unexpectedly, a signal is not received from one of the units 2, 4, 6, each of the processors 12 within the security system causes the alarm 16 to be activated. Also, if one particular unit does not receive any signals from the remaining units (eg it is the unit that has been removed/stolen) it will sound its alarm 16. Therefore, if, as in this example, a unit 2, 4, 6 is attached to a number of suitcases the alarm will sound on each of the suitcases. To improve tolerance to false alarms there may be

more than one missed communication before the processor causes an alarm to be generated.

Such a system may be beneficial if a user were travelling with a number of suitcases. By providing a unit according to the invention on each of the cases, the cases would effectively guard one another. If one of the cases were stolen, and moved out of the transmitting range of the other units, then the alarm 16 would sound on each of the cases; on the stolen case and on the ones which were not stolen.

If the system is left active for a long period it is possible for the battery 18 to fail. Clearly, should the battery fail within a particular unit then that unit will no longer be capable of transmitting a signal. This situation would be analogous to the unit being stolen and being moved out of transmission range. Therefore, in this particular embodiment the battery 18 status is transmitted within the signal. If a particular unit has been reporting a low battery 18 status for a period of time then the remaining units of the system do not activate the alarm 16 if that particular unit suddenly stops transmitting. The remaining units effectively realise that the battery 18 of the particular unit has failed.

It is conceivable that one of the units may be on the fringes of transmission range of the transmitters 8 and therefore experience unreliable communication with the units of the system. In such circumstances the other units may note the unreliable nature of the communication and consequently ignore the unit experiencing unreliable communication. The signal output by the RSSI output of the receiver 10, or an ongoing measure of the Bit Error Rate, may be used to determine the reliability of the transmission. This will help to prevent false alarms. Clearly, if a unit is experiencing communication difficulties from the time that the system is armed it is likely to trigger a false alarm due to missed transmissions or transmission. In one particular embodiment the units may estimate the range of other units based upon the received signal strength. If the estimated range is above a threshold limit that particular unit may be discounted. Of course, other units may still be in range of that

particular unit and continue to guard that unit. A user of the system may be provided with a warning that a unit is "out of range" allowing the user to move that particular unit.

In a further embodiment in which an alarm is raised if communication is lost with any particular unit, as shown in Figure 3, an anchor unit 20 (or base station) is provided on a substantially permanent structure 22, in this case a pillar. It will be appreciated that should a number of highly mobile objects (for example a number of suitcases 24, 26, 28 each fitted with a unit 30, 32, 34) which are guarded by the security system all be stolen together, then the alarms 16 will not be activated; the units 30, 32, 34 will remain in communication with one another and will therefore not realise that anything is amiss.

However, the provision of the anchor unit 20 on the pillar 22 ensures that not all of the units of the system can be stolen, and removed, at the same instance. Should all of the suitcases 24, 26, 28 be stolen together, the units 30, 32, 34 would still each remain in communication, but each of those units (30, 32, 34) would lose communication with the anchor unit 20. Because communication with one of the units has been lost then all of the alarm means 16 would be activated. Fixed units such as anchor unit 20 may be provided in public areas so that users of the security system can guard articles fitted with the security system. Of course, more than one anchor 20 could be provided.

Yet another embodiment of the invention is shown in Figure 4 wherein a master unit 36 is provided. In this embodiment the master unit 36 and the remaining units 38, 40, 42 are not identical as with the other embodiments so far described. The master unit 36 can be used to control the security system and is provided with a display 44 and an alarm 46. The remaining units 38, 40, 42 are not provided with alarms (although of course they could be) but are provided with key-receiving mechanisms. An arming mechanism 48 is also provided on the master unit. (The master unit may be thought of as an arming unit).

The display is adapted in this embodiment to display the status of units within the security system and in this embodiment comprises an LCD display. The display 44 may function in conjunction with an input device (not shown) so that the user can manipulate the display so that the desired information is displayed on the display 44.

In this embodiment the whole system can be armed by the use of the arming mechanism 48. When the arming mechanism 48 is activated the master unit 36 transmits an arming code or key to the remaining units 38, 40, 42 which is received by the receiver and the key-receiving mechanism. The units start periodically to transmit signals as described in relation to Figures 1 and 3. In this embodiment, if communication is lost with any one of the units 36, 38, 40, 42, a signal propagates back to the master unit that the alarm 46 is activated. The master unit 36 and other units change the arming code after each use according to a predetermined sequence so that the code cannot be fraudulently copied.

Providing a master unit 36 in this manner allows the remaining units 38, 40, 42 to be made simpler and cheaper, whilst maintaining the functionality of the system.

In a slight modification of this embodiment the master unit 36 is not provided with a physical arming mechanism 48 which must be activated, neither is the master unit 36 the only unit provided with an alarm (each unit being provided with its own alarm). In this embodiment the master unit 36 periodically transmits a suppression signal which is received by the remaining units 38, 40, 42. As long as the remaining units 38, 40, 42 receive the suppression signal the system remains unarmed. As soon as reception of the suppression signal by the remaining units 38, 40, 42 is lost or the distance exceeds a given value, the system becomes armed, this reception acting as the arming mechanism. Once armed, should communication be lost between any of the remaining units 38, 40, 42, then the alarm of each of the remaining units 38, 40, 42 is activated.

Such an embodiment is useful because it provides for automatic arming of the system. Using the example of a collection of suitcases fitted with the security system the master unit 36 would be carried by the person in charge of the cases. Whilst that person is carrying the cases there is no need for the system to be armed, and indeed in this embodiment the system would not be armed because each of the units on the cases would be in communication with the master unit and receive the suppression signal.

When the cases are left unattended it is desirable for them to be guarded. In this embodiment the system would automatically arm when the cases are left by the person looking after them and would guard one another.

In an alternative embodiment, not shown, each of the units of the system is provided with an arming mechanism. In use, a user activates the arming mechanism on each of the units of the system in order to activate the security system.

In another embodiment the units of the system will only remember the identities of units which start communication within a predetermined period of the system being activated. This will prevent the units from guarding units which are not part of that particular security system. For instance, if two groups of suitcases were each fitted with units according to the invention, then each suitcase within each group would guard each of the others. If, however, the two groups were brought into close proximity and the units simply guarded any unit with which they were in communication, then the units of the two groups would start guarding each other. Therefore, when the two groups were again separated the alarms of the units would be activated. Programming the units to guard only those units which are in communication with each other within a predetermined arming period would overcome this problem.

In its widest concept the basic algorithm of the security system may be thought of as "when armed, detect all other units and then generate an alarm if predetermined

circumstances occur (or predetermined rules are satisfied)". Thus, as discussed in the preceding paragraph, this may cause the system to guard units which it should not be guarding. Causing the units to remember the units which they should guard may be likened to a teaching phase.

In one embodiment the predetermined rules may require that an alarm be generated if communication is lost with any unit of the systems. Such rules are useful as described in the embodiment described above.

In another embodiment, the rules may require that an alarm is generated if communication is received from a unit or too many units. Generation of an alarm by too many units may be useful for preventing overcrowding, perhaps in lifts or other confined spaces.

The skilled person will appreciate that the rules which govern whether or not an alarm is generated can be arbitrarily complex and based on any number of circumstances.

In another embodiment an alarm may be generated if a unit becomes present. Such a system would be useful for enforcing exclusion orders. A unit may generate an alarm should a unit having a particular unique identity or class of membership be detected.

In alternative embodiments different methods of programming the units to know which units form the system may be provided. For instance, one or more of the units may be provided with an input device which in one embodiment is a button. When the button is pressed the units forming the system remember the identities of each of the units with which they are in communication. Once the button is released the units will not start to guard other units and will only guard those units which they have been in communication with when the button was pressed.

Alternatively, the input means may be a keyboard, a collection of keys, or other data input devices which can be used to input the identity of the units which those particular units should guard.

In some embodiments the input device allows the rules which govern whether or not an alarm is generated to be altered, thus changing the functionality of the system. The rules may also be modified following communication from other units providing instructions to change the rules.

The rules governing whether or not an alarm is generated may be arbitrarily complex, and may comprise Boolean or arithmetical expressions based on any number of variables. Variables may include the state of sensors, the received signal strength, the measured distance, the presence or absence of particular units with a unique identification or class, time, etc. [Each unit may be provided with a clock.]

Sensors may be provided as an input to the processors of the units. Such sensors allow the unit to be aware of its surroundings and may be used to generate alarms based on readings from the sensors. Examples of sensors which may be provided include: tamper-switches, continuity-loop sensor wires from external alarm systems (e.g. Volumetric™), signals sent from a computer program running on an attached computer, signals sent from a co-located passive "RFID" chip, co-ordinates from a GPS positioning sensor, signals from a telephone (including mobile) and including the ringing signal, moisture sensors, motion and tilt sensors, magnetic field sensors including compasses, biometric sensors and physiological sensors.

The key receiving mechanism on the arming units may receive mechanical keys rather than an electronic code to arm the units.

In one embodiment one of the units is provided with a connector which allows the security system to interface with an external piece of apparatus. The external piece of apparatus may be a computer network, a telephone, a visual display unit (or other

display), a portable computing device, a mobile phone network, a door lock, a turnstile, another security system, or some other device. Such a connector allows the status of the system to be observed.

In the embodiments discussed above, it is disclosed to transmit the identity of a particular unit. In other embodiments the identity of the unit may not form part of the transmission. In some embodiments the processor may be adapted to cause the transmitter to transmit a predetermined class to which that particular unit has been designated.

Not transmitting a unique identification is advantageous in some circumstances because it will prevent abuse of user's privacy wherein the transmissions could be used to track a particular unit if a unique identification is transmitted. Transmitting a predetermined class would not allow a particular unit to be tracked.

Further, having predetermined classes to which units belong may provide functionalities which although possible by transmitting a unique identification may be easier to implement by transmitting a class. Indeed, in some embodiments a portion of the unique identification may comprise a class, or a class may be transmitted in addition to the unique identification.

Examples of uses relying on a class to be transmitted include providing children with units which transmit membership of a "child" class. Units provided on turnstiles may receive communications from the units, identify that they belong to the "child" class and only allow them to pass if a unit belonging to an "adult" class is also present. Further, guns may be provided with units which only operate when they detect a communication from a unit belonging to a "firing range" class.

A class based system could be used to guard a building where units in the vicinity of an entrance produce an alarm if a unit belonging to the class "asset" (which is attached to a company asset) leaves the building without there also being present a

unit belonging to the class "employee". The skilled person will appreciate that the use of such classes has many uses. A further example would be restricting access to a secure piece of equipment which requires two people to be present. People could be issued with a unit belonging to a "person" class and the equipment may only become operational if a unit attached to it detects two units of the "person" class.

Class of membership (unlike unique identifications) are not specific to individual units and therefore this class of membership is harder to use to invade privacy.

In some embodiments the processing means stores within the memory a log of events which the unit has experienced. This log can be accessed via communications with other units or via the connector.

An example of a circuit for providing a unit is shown in Figure 2. The power supply (not shown) is connected to the terminals BAT1, BAT2, and the section labelled A smoothes, filters and regulates this power supply.

The circuit section labelled B is a transmitter, which is driven by a pin 6 of U1. The receiver of the unit is provided by section C. The majority of section D provides the processing power of the circuit. However, a battery low sensor is provided by the Zener diode and resistor pair at E. An LED F provides an output to the unit, and a push button switch G provides an input. Also, a piezo sounder H provides an alarm.

A table showing the component values for the circuit now follows:

Component	Value	Component	Value
R_1	2.2kΩ	C_4	0.47µF
R_2	10Ω	C_5	22µF
R_3	100kΩ	C_6	22µF
R_4	22kΩ	C_7	0.47µF
R_5	100kΩ	VC_1	10pF
R_6	56kΩ	L_1	Not fitted
R_7	22kΩ	L_2	15nH
R_8	0Ω	X_1	3.36MHz
R_9	1.0kΩ	U_1	PICI6C505-04IP
R_{10}	680Ω	U_2	MICRF001
C_1	0.1µF	U_3	LM2391Z.5
C_2	10nF	TX_1	LPRSTX
C_3	22µF		

CLAIMS:

1. A security system comprising at least two units, each unit comprising a power source adapted to power the unit, a processor, a transmitter, a receiver and at least one of the units having an alarm, the units having the ability to communicate with each other via the transmitters and receivers, the processors being adapted to control the units and to cause the alarm to generate an alarm signal when predetermined rules are satisfied.

2. A system as claimed in claim 1, wherein at least one but not all of the units is provided with an alarm.

3. A system as claimed in claim 1 or 2, wherein all of the units are provided with an alarm.

4. A system as claimed in claim 1, 2 or 3, wherein the alarm on every unit provided with an alarm is caused to generate an alarm signal when a predetermined rule is satisfied.

5. A system as claimed in any preceding claim, wherein the transmitter of at least one of the units is adapted periodically to transmit a signal.

6. A system as claimed in any preceding claim, wherein the receiver of at least one of the units is activated periodically so as periodically to be capable of receiving a signal.

7. A system as claimed in claim 5 or 6, wherein the processor of at least one of the units is adapted to operate the transmitter of that unit so as to transmit a signal only when the receiver of another unit is activated to receive a signal.

8. A system as claimed in claim 5, 6 or 7, wherein the processor of at least one

of the units is adapted to operate the receiver of that unit so as to be capable of receiving a signal only when the transmitter of another unit is activated to transmit a signal.

9. A system as claimed in any one of claims 5 to 8, wherein the processor of at least one of the units is adapted to learn when a transmission is expected from another unit and to operate the receiver of the at least one unit accordingly.

10. A system as claimed in any preceding claim, wherein at least one of the units is adapted to operate in a low power state until a possible communication is detected by the receiver, in which event the at least one unit is adapted to become fully operational.

11. A system as claimed in claim 10, wherein the at least one unit is adapted to become fully operational for a predetermined time upon detection of a possible communication, returning to the low power state upon elapse of the predetermined period of time.

12. A system as claimed in claim 10 or 11, wherein the at least one unit is adapted to return to a low power state upon detection of an appropriate communication.

13. A system as claimed in any preceding claim, wherein at least one of the units is provided with an identification mechanism adapted to provide unit identity.

14. A system as claimed in claim 13, wherein the processor of the at least one unit is adapted to interact with the identification mechanism so as to transmit a unit identity by way of the transmitter of that at least one unit.

15. A system as claimed in claim 14, wherein the identification mechanism is an integral part of the processor.

16. A system as claimed in any one of claims 13 to 15, wherein the identification mechanism provides a unique identification code for each unit provided therewith.

17. A system as claimed in any one of claims 13 to 16, wherein the identification mechanism provides an identification code that identifies each unit provided therewith as belonging to a predetermined class of units.

18. A system as claimed in any preceding claim, wherein at least one of the units is provided with an arming mechanism adapted to arm the unit by causing it to become fully operational.

19. A system as claimed in claim 18, wherein the arming mechanism is further adapted to disarm the unit by causing it to enter into a dormant or low power state.

20. A system as claimed in claim 18 or 19, wherein the arming mechanism includes a key-receiving mechanism adapted to receive a key.

21. A system as claimed in claim 20, wherein the key-receiving mechanism is adapted to receive a key selected from the group comprising: an electronic key such as a smart card or the like, a mechanical key and an arming code transmitted to the at least one unit and received by the receiver thereof.

22. A system as claimed in any one of claims 18 to 21, wherein at least one of the units comprises an arming unit adapted to arm the system as a whole.

23. A system as claimed in claim 22, wherein the arming unit is adapted to transmit an arming code that arms and/or disarms the remaining units of the system.

24. A system as claimed in claim 22 or 23, wherein at least one of the units is adapted to transmit a suppression signal adapted to prevent the remaining units of the

system from arming.

25. A system as claimed in claim 24, wherein the remaining units of the system become armed if the suppression signal is not detected for a predetermined period of time.

26. A system as claimed in claim 22 or 23, wherein at least one of the units is adapted to transmit a suppression signal adapted to prevent the remaining units of the system from disarming.

27. A system as claimed in claim 26, wherein the remaining units of the system become armed if the suppression signal is not detected for a predetermined period of time.

28. A system as claimed in claim 23 or any one of claims 24 to 27 depending from claim 23, wherein the arming unit is adapted periodically to change the arming code.

29. A system as claimed in any preceding claim, wherein communications between the units are encrypted.

30. A system as claimed in any preceding claim, wherein at least one of the units is provided with a memory.

31. A system as claimed in claim 30 depending from claim 13 or any claim dependent therefrom, wherein the processor of the at least one unit is adapted to store within the memory the identity of at least one further unit with which it is in communication.

32. A system as claimed in claim 30 or 31, wherein the processor of the at least one unit is adapted to store a log of events within the memory.

33. A system as claimed in any one of claims 30 to 32, wherein the processor of the at least one unit is adapted to cause the transmitter of that unit to transmit all or some of the contents of the memory.

34. A system as claimed in claim 31 or any claim dependent therefrom, wherein the processor of the at least one unit is adapted to store within the memory only the identity of at least one further unit with which it is in communication at a predetermined time or within a predetermined period of time.

35. A system as claimed in any preceding claim, wherein the processor of at least one of the units is adapted to generate an alarm when communication fails between that unit and at least one other of the units.

36. A system as claimed in claim 13 or any claim dependent therefrom, wherein the processor of at least one of the units is adapted to generate an alarm if a communication is received from at least one other unit having a predetermined identity or belonging to a class of units having a predetermined identity.

37. A system as claimed in claim 13 or any claim dependent therefrom, wherein the processor of at least one of the units is provided with an input device adapted to program the processor with the identity or identities of other units which are part of the system.

38. A system as claimed in claim 37, wherein the identity or identities of the other units is or are stored in a memory of the at least one unit when the input device is activated.

39. A system as claimed in any preceding claim, wherein at least one of the units is provided with at least one sensor having an output connected to the processor.

40. A system as claimed in claim 39, wherein the processor of the at least one unit is adapted to monitor the output of the at least one sensor and to cause information relating to the sensor output to be transmitted by the transmitter.

41. A system as claimed in claim 39 or 40, wherein the sensor is selected from the group comprising: moisture sensors, motion/tilt sensors, tamper switches, continuity-loop sensor wires from external alarm systems, a computer program running on an attached computer, RFID chips, Global Positioning sensors, mobile telephones, magnetic field sensors including compasses, biometric sensors and physiological sensors.

42. A system as claimed in any preceding claim, wherein at least one of the units is provided with a connector to connect the unit with apparatus remote from the system.

43. A system as claimed in claim 42, wherein the connector is adapted to allow communication with at least one member of the group comprising: a video display, a website, a telephone system, an external computer, a computer network, a portable computing device, a mobile telephone network, a door lock, a turnstile and another security system.

44. A system as claimed in claim 42 or 43, wherein the connector is adapted to make available information regarding a status of the system.

45. A system as claimed in any one of claims 42 to 44 depending ultimately from claim 30, wherein the connector is adapted to transmit the contents of the memory.

46. A system as claimed in any one of claims 42 to 45 depending ultimately from claim 32, wherein the connector is adapted to transmit the contents of the log of events.

47. A system as claimed in any preceding claim, wherein at least one of the units is provided with an attachment device adapted to attach the unit to an object to be guarded.

48. A system as claimed in any preceding claim, wherein at least one of the units is attached to or incorporated into a substantially permanently fixed structure so as to constitute an anchor unit.

49. A system as claimed in any preceding claim, wherein the transmitter is adapted to provide a modulation format selected from the group comprising: on-off keying, amplitude shift keying, frequency shift keying, frequency modulation, amplitude modulation, frequency hopping, spread spectrum and time-modulated ultra-wide band.

50. A system as claimed in any preceding claim, wherein the transmitter and receiver are provided together as a transceiver.

51. A system as claimed in any preceding claim, wherein at least one of the units is provided with at least one antenna for transmitting and/or receiving radio signals.

52. A system as claimed in claim 51, wherein the at least one unit is provided with at least two antennas.

53. A system as claimed in claim 52, wherein the at least two antennas are disposed in a mutually substantially orthogonal configuration.

54. A system as claimed in claim 52 or 53, wherein the at least two antennas are spaced from each other.

55. A system as claimed in any one of claims 52 to 54, wherein the at least two antennas are used alternatively for transmission and reception.

56. A system as claimed in claim 52, wherein the at least two antennas form an array of antennas having "beam-forming" or "radio direction finding" (RDF) directional properties.

57. A system as claimed in any preceding claim, wherein there is provided more than two units, and wherein each unit is able to communicate with every other unit in the system.

58. A system as claimed in any preceding claim, wherein the transmitter at least one of the units is adapted to transmit pieces of information selected from the group comprising: an identity of the unit, a class of the unit, a status of the unit, an indication of when a next transmission will be transmitted by the unit.

59. A system as claimed in any preceding claim, wherein the transmitter of at least one of the units as adapted to transmit information regarding a level of output from the power source of the unit.

60. A system as claimed in claim 59, wherein the processor of at least one of the units is adapted to suppress the generation of an alarm if communications are not received from another unit that has been reporting low power levels for a predetermined period.

61. A system as claimed in any preceding claim, wherein the transmitters and receivers are adapted to communicate by way of radio signals.

62. A system as claimed in claim 61, wherein the transmitters and receivers have a range of 1m to 150m.

63. A system as claimed in claim 61, wherein the transmitters and receivers have a range of 30m to 125m.

64. A system as claimed in claim 61, wherein the transmitters and receivers have a range of 5m.

65. A system as claimed in claim 61, wherein the transmitters and receivers have a range of 10m.

66. A system as claimed in claim 61, wherein the transmitters and receivers have a range of 20m.

67. A system as claimed in claim 61, wherein the transmitters and receivers have a range of 1km.

68. A system as claimed in claim 61, wherein the transmitters and receivers have a range of 5km.

69. A system as claimed in claim 61, wherein the transmitters and receivers are adapted to operate at a frequency of substantially 433MHz.

70. A method of providing security comprising providing at least two units capable of communicating with each other using transmitters and receivers, the method comprising sending communication signals between the at least two units and raising an alarm when predetermined rules are satisfied.

71. A method according to claim 70, wherein an alarm is generated when communication fails between at least two units.

72. A method according to claim 70 or 71, wherein the units are armed and/or disarmed by way of an arming mechanism.

73. A method according to claim 72, wherein the units are prevented from arming through the transmission of a suppression signal from a predetermined master unit.

74. A method according to claim 73, wherein the units become armed in the absence of the suppression signal.

75. A method according to any one of claims 70 to 74, wherein the units perform a communications check to establish that each unit is in communication with at least one other unit.

76. A method according to any one of claims 72 to 75, wherein at least one of the units is caused to remember an identity of each other unit with which it is in communication when the units are armed or within a predetermined time therefrom.

77. A method according to any one of claims 70 to 76, wherein at least one of the units is provided with an input device which is operable to input an identity of each other unit with which the at least one unit is intended to be in communication.

78. A method according to any one of claims 70 to 77, wherein at least one of the units is provided with an input device and wherein each of the units remembers with which other units it is in communication when an input is made to the input device.

79. A method according to any one of claims 70 to 78, wherein the units are caused to transmit signals only at predetermined periods of time.

80. A method according to any one of claims 70 to 79, wherein the units are operable to receive signals only at predetermined periods of time.

81. A method according to any one of claims 70 to 80, wherein each unit is operable to transmit information regarding a status of the unit.

82. A method according to claim 81, wherein the information includes the status of a power source of the unit.

83. A method according to claim 82, wherein an alarm signal is suppressed if a unit stops transmitting after a predetermined period of reporting a low power source.

84. A method according to any one of claims 70 to 83, wherein a signal strength of received transmissions is noted.

85. A method according to claim 84, wherein an alarm signal is suppressed if no signal is received from a unit that has been noted to have a weak signal strength for a predetermined period of time.

86. A method according to any one of claims 70 to 85, wherein at least one of the units estimates its distance from each of the other units with which it is in communication.

87. A method according to claim 86, wherein the estimation is performed by measuring received signal strength.

88. A method according to claim 86 or 87, wherein at least one of the units is caused to ignore signals from units which are more than a predetermined distance therefrom.

89. A method according to claim 84 or any claim dependent therefrom, wherein a warning is issued to a user if one of the units is experiencing a weak signal strength.

90. A method according to claim 86 or any claim dependent therefrom, wherein a warning is issued to a user if a unit is estimated to be greater than a predetermined distance from the at least one unit.

91. A method according to claim 76 or 77 or any claim dependent therefrom, wherein an alarm is generated if the at least one unit receives a signal from a unit having a predetermined identity.

92. A method according to claim 76 or 77 or any claim dependent therefrom, wherein an alarm is generated if the at least one unit receives a signal from a unit having an unknown identity.

93. A security unit comprising:

a transmitter for transmitting a signal;

a receiver for receiving such a signal when transmitted by a second, substantially identical, unit;

an alarm generator; and

a processor adapted to activate the alarm generator according to a predetermined condition relating to the receipt or otherwise of a said signal.

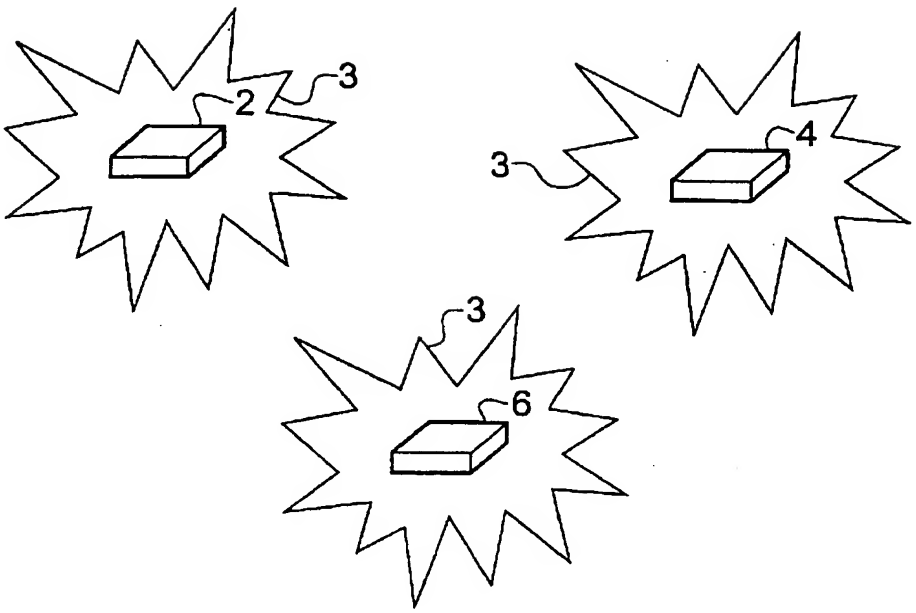


Fig. 1

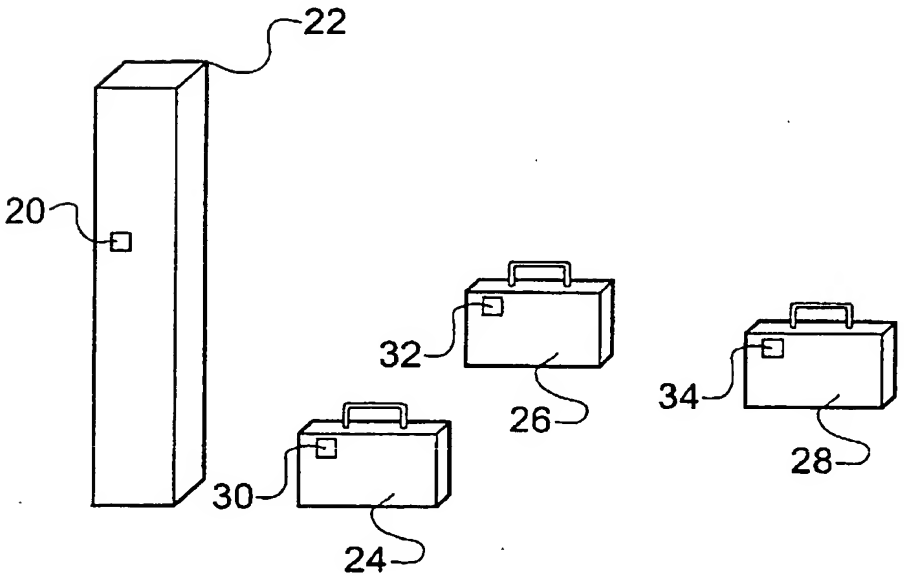


Fig. 3

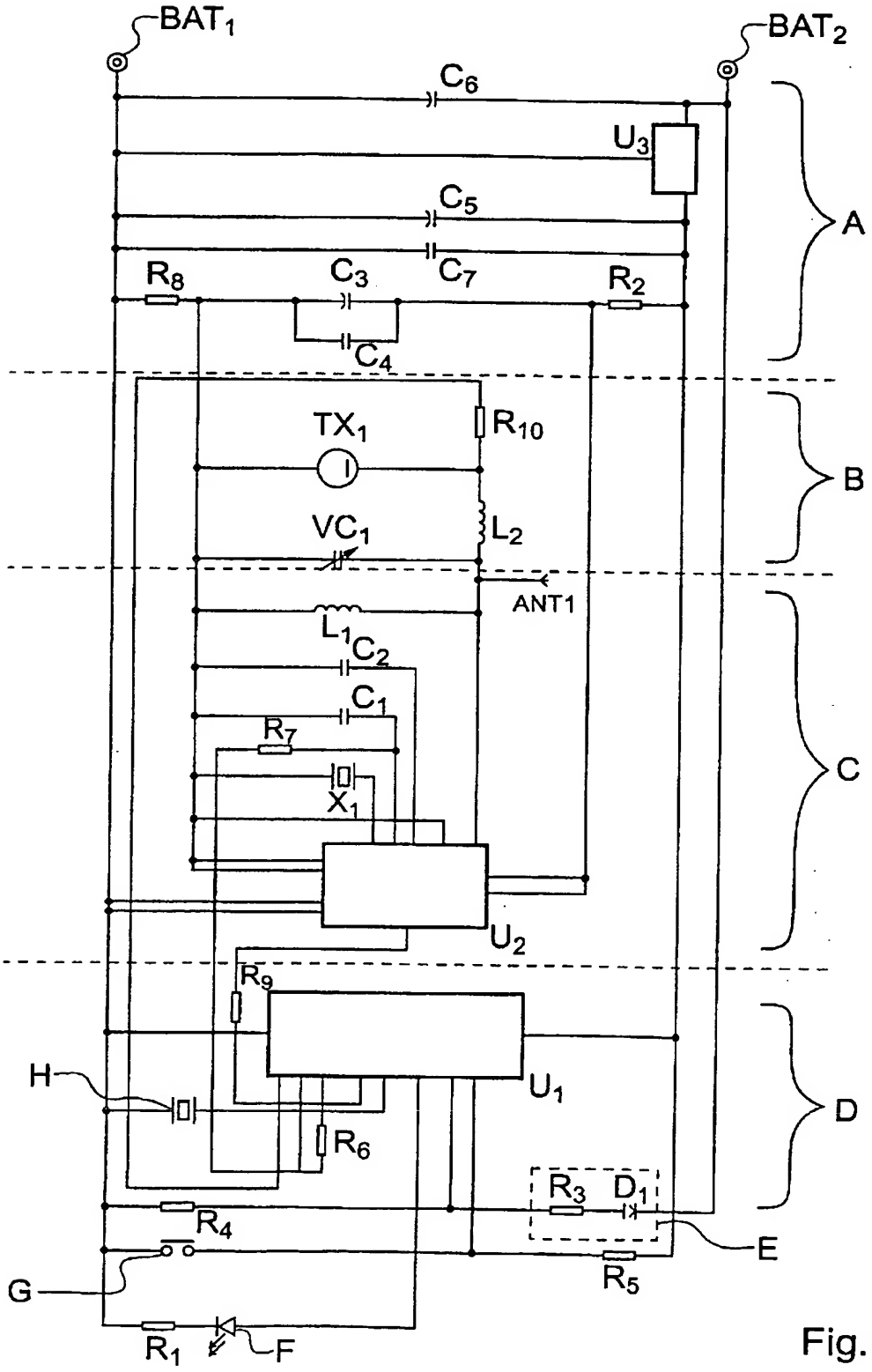

BAT1
BAT2
C6
U3
C5
C7
R8
C3
R2
C4
A
TX1
R10
B
VC1
L2
ANT1
L1
C2
C1
R7
X1
C
U2
R9
U1
H
R6
D
R3
D1
R4
E
G
R5
R1
F

Fig. 2

3/3

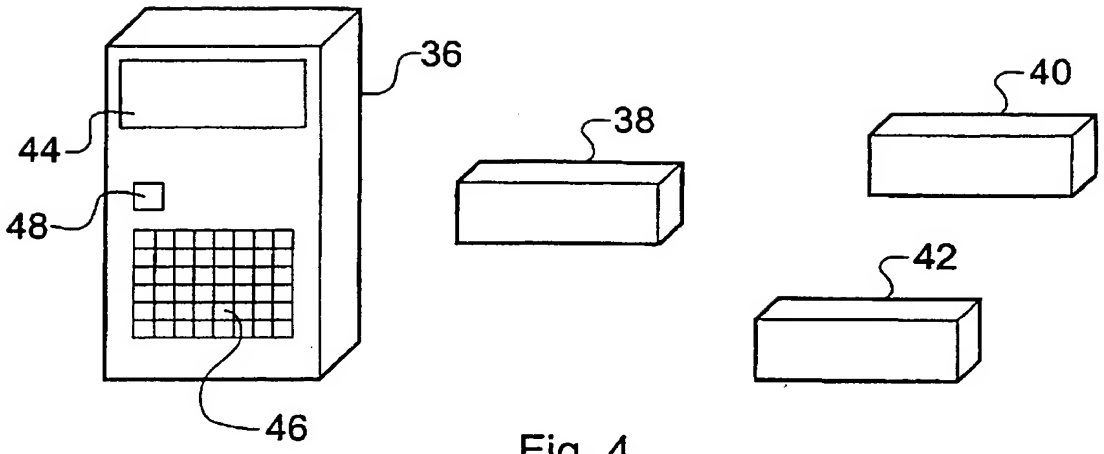


Fig. 4

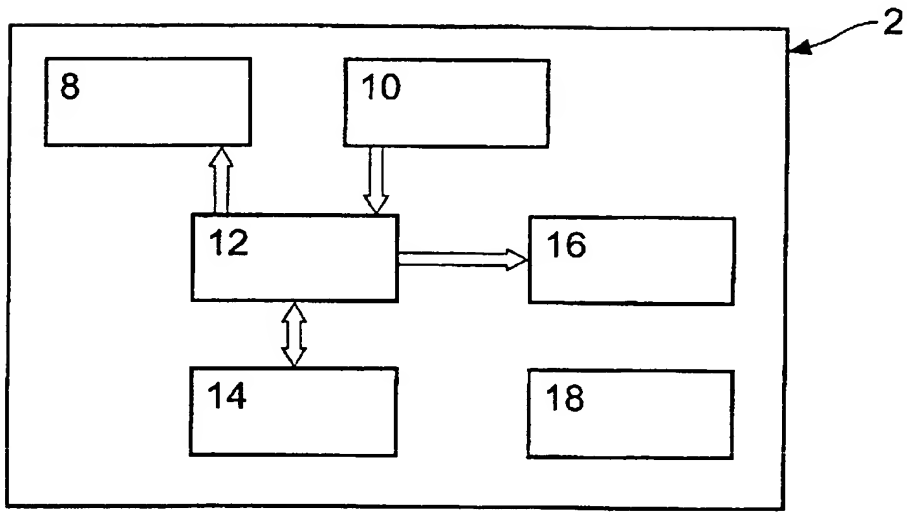


Fig. 5